

A GENERALIZATION OF REDUCED ARAKELOV DIVISORS OF A NUMBER FIELD

HA THANH NGUYEN TRAN

ABSTRACT. Let $C \geq 1$. Inspired by the LLL-algorithm, we define strongly C -reduced divisors of a number field F which are generalized from the concept of reduced Arakelov divisors. Moreover, we prove that strongly C -reduced Arakelov divisors still retain outstanding properties of the reduced ones: they form a finite, regularly distributed set in the Arakelov class group and the oriented Arakelov class group of F .

1. INTRODUCTION

Let F be a number field of degree n . The Arakelov class group Pic_F^0 of F is an analogue of the Picard group of an algebraic curve. Computing this group is of interest since one can read off the class number and the unit group of F from it (see [2, 4, 6, 9]). A good tool to compute Pic_F^0 is the *reduced Arakelov divisors* the theory of which is also called *infrastructure* of F (see [3, 8, 11]). The set of these reduced Arakelov divisors has a group-like structure that enables to obtain a reduced divisor by performing reduction on the sum of two reduced divisors. This phenomenon was first discovered through computing regulators of real quadratic fields (see [8]).

Reduced Arakelov divisors form a finite and regularly distributed set in Pic_F^0 (see Section 7 in [7] and Chapter 1 in [9]). Therefore, for any class of divisors D of Pic_F^0 , we can always find a reduced divisor D' that is close to D and use it to compute at D . There is an effective method to find such a reduced divisor D' [7, Algorithm 10.3]. However, this algorithm requires finding a shortest vector of the lattice associated to D which is a very time-consuming process. On the other hand, computing a reasonable short vector, such as using the LLL-algorithm, is much faster and easier than finding a shortest vector. This leads to modifications and generalizations of the concept of reduced divisors to C -reduced divisors.

The first the generalization is proposed by Schoof (see [9, Chapter 2] and [10]) which is called *C -reduced Arakelov divisor*. However, for general number fields, it is unknown how to efficiently test whether a given divisor is C -reduced. This paper focuses on the second generalization – *strongly C -reduced Arakelov divisors*. It is inspired by the properties of LLL-reduced bases of the lattices associated to Arakelov divisors.

With this definition, testing whether a given divisor is strongly C -reduced can be done in time polynomial in $\log(|\Delta_F|)$, where Δ_F is the discriminant of F (see Section

Key words and phrases. Arakelov divisor, reduced, C -reduced, strongly C -reduced, infrastructure, Arakelov class group.

3.3 in [9] for more details). Especially, the LLL-algorithm yields strongly C -reduced Arakelov divisors with $C = \sqrt{n} 2^{(n-1)/2}$ (see Example 3.2).

Strongly C -reduced divisors are C -reduced (see [10]). In addition, a reduced divisor in the usual sense is strongly C -reduced with $C = \sqrt{n}$ and a strongly C -reduced divisor is reduced in the usual sense with $C = 1$. Furthermore, strongly C -reduced divisors still admit the same remarkable properties as reduced divisors in the sense that they form a finite and regularly distributed set in Pic_F^0 . These are the most important results of this paper presented in Theorem 4.5, 4.6 and 4.8.

In Section 2, we briefly recall some definitions and basic properties of Arakelov divisors. Section 3 introduces strongly C -reduced divisors and their properties are provided in Section 4.

2. PRELIMINARIES

This section is devoted to introducing Arakelov divisors and reduced Arakelov divisors of a number field F . The Arakelov class group and the oriented Arakelov class group as well the metrics on these groups are briefly recalled. All details can be found in [7] and [9].

Let F be a number field of degree n and r_1, r_2 the number of real and complex infinite primes (or infinite places) of F .

2.1. Arakelov divisors and reduced Arakelov divisors.

Let $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{\sigma \text{ complex}} \mathbb{C}$ with σ running over the infinite primes of F . Then $F_{\mathbb{R}}$ is an étale \mathbb{R} -algebra with a canonical Euclidean structure given by the scalar product

$$\langle u, v \rangle := \text{Tr}(u\bar{v}) \text{ for any } u = (u_{\sigma}), v = (v_{\sigma}) \in F_{\mathbb{R}}.$$

Here and in the rest of the paper we often call fractional ideals simply ‘ideals’. To emphasize that an ideal is integral, we call it an integral ideal.

Definition 2.1. An *Arakelov divisor* is a formal finite sum $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_{\sigma} \sigma$ where \mathfrak{p} runs over the nonzero prime ideals of O_F and σ runs over the infinite primes of F , here the coefficients $n_{\mathfrak{p}}$ are in \mathbb{Z} but the x_{σ} can be any number in \mathbb{R} .

The set of all Arakelov divisors of F is an additive group denoted by Div_F . The degree of an infinite prime σ is equal to 1 or 2 depending on whether σ is real or complex. The degree of D is $\deg(D) := \sum_{\mathfrak{p}} n_{\mathfrak{p}} \log N(\mathfrak{p}) + \sum_{\sigma} \deg(\sigma) x_{\sigma}$.

Let I be a fractional ideal of F . Then each element g of I is mapped to the vector $(\sigma(g))_{\sigma}$ in $F_{\mathbb{R}}$ by the infinite primes σ . For any vector $u = (u_{\sigma})_{\sigma}$ in $F_{\mathbb{R}}$ and any $g \in I$, the vector $ug = (u_{\sigma} \sigma(g))_{\sigma}$ is in $F_{\mathbb{R}}$, so then

$$\|ug\|^2 = \sum_{\sigma \text{ real}} u_{\sigma}^2 |\sigma(g)|^2 + 2 \sum_{\sigma \text{ complex}} |u_{\sigma}|^2 |\sigma(g)|^2.$$

To every Arakelov divisor D as in Definition 2.1, there corresponds a *Hermitian line bundle* (I, u) where $I = \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$ a fractional ideal of F and $u = (e^{-x_{\sigma}})_{\sigma}$ a vector in $\prod_{\sigma} \mathbb{R}_{+}^{*}$. This correspondence is bijective and we often identify the two notions.

Additionally, we associate to D the *lattice* $L = uI = \{uf : f \in I\} \subset F_{\mathbb{R}}$ with the inherited metric from $F_{\mathbb{R}}$ (see more about ideal lattices in [1]). The covolume of this lattice $L = uI$ is $\text{covol}(L) = \sqrt{|\Delta|}e^{-\deg(D)}$. We define $\|f\|_D^2 := \|uf\|^2$ for all $f \in I$.

For each element $f \in F^*$, the *principal* Arakelov divisor (f) is the Arakelov divisor of Hermitian line bundle $(f^{-1}O_F, |f|)$ where $f^{-1}O_F$ is the principal ideal generated by f^{-1} and $|f| = (|\sigma(f)|)_{\sigma}$. The product formula implies that $\deg((f)) = 0$ for all $f \in F^*$.

Definition 2.2. Let I be a fractional ideal of F . An element f in I is called *minimal* if for all $g \in I$ if $|\sigma(g)| < |\sigma(f)|$ for all σ then $g = 0$.

Definition 2.3. Let I be a fractional ideal of F . We define $d(I)$ to be the divisor (I, u) with $u = (u_{\sigma})_{\sigma}$ and $u_{\sigma} = N(I)^{-1/n}$ for all σ .

Definition 2.4. A fractional ideal I is called *reduced* if 1 is minimal in I . An Arakelov divisor D is called *reduced* if D has the form $D = d(I)$ for some reduced fractional ideal I .

2.2. The Arakelov class group.

The set of all Arakelov divisors of degree 0 form a group, denoted by Div_F^0 . It contains the subgroup of principal divisors. Similar to an algebraic curve, we have the following definition.

Definition 2.5. The *Arakelov class group* Pic_F^0 of F is the quotient of Div_F^0 by its subgroup of principal divisors.

Denote by $(\oplus_{\sigma}\mathbb{R})^0 = \{(x_{\sigma}) \in \oplus_{\sigma}\mathbb{R} : \sum_{\sigma} \deg(\sigma)x_{\sigma} = 0\}$ and $\Lambda = \{(\log|\sigma(\varepsilon)|)_{\sigma} : \varepsilon \in O_F^*\}$. Then Λ is contained in the vector space $(\oplus_{\sigma}\mathbb{R})^0$. Let

$$T^0 = (\oplus_{\sigma}\mathbb{R})^0 / \Lambda.$$

Then by Dirichlet's unit theorem, T^0 is a compact real torus of dimension $r_1 + r_2 - 1$ [8, Section 4.9]. Each $(x_{\sigma}) \in T^0$ is mapped to the class of divisors $(O_F, (e^{-x_{\sigma}}))$ in Pic_F^0 . In this way, T^0 becomes a subgroup of Pic_F^0 . Denoting by Cl_F the class group of F , the structure of Pic_F^0 can be seen by the proposition below.

Proposition 2.6. *Mapping a divisor class (I, u) to the class of ideal I induces the following exact sequence.*

$$0 \longrightarrow T^0 \longrightarrow \text{Pic}_F^0 \longrightarrow Cl_F \longrightarrow 0.$$

Proof. See [7, Proposition 2.2]. □

For $u \in \prod_{\sigma} \mathbb{R}_{>0}$, we let $\log u$ denote the element $\log u := (\log(u_{\sigma}))_{\sigma} \in \prod_{\sigma} \mathbb{R} \subset F_{\mathbb{R}}$. By using the scalar product from $F_{\mathbb{R}}$, this vector has length $\|\log u\|^2 = \sum_{\sigma} \deg(\sigma) |\log(u_{\sigma})|^2$. So, we define

$$\|u\|_{Pic} = \min_{\substack{u' \in \prod_{\sigma} \mathbb{R}_{>0} \\ \log u' \equiv \log u \pmod{\Lambda}}} \|\log u'\| = \min_{\varepsilon \in O_F^*} \|\log(|\varepsilon|u)\|.$$

Now let $[D]$ and $[D']$ be two classes containing divisor D and D' respectively and lying on the same connected component of Pic_F^0 . Then by Proposition 2.6, there is some

unique $u \in T^0$ such that $D - D' = (O_F, u)$. We define the *distance* between 2 divisor classes containing D and D' as $\|u\|_{Pic}$.

The function $\| \cdot \|_{Pic}$ gives rise to a distance function that induces the natural topology of Pic_F^0 [7, Section 6].

2.3. The oriented Arakelov class group.

Definition 2.7. An *oriented Arakelov divisor* is a pair (I, u) where I is a fractional ideal and u is an arbitrary unit in $F_{\mathbb{R}}^*$.

The degree of an oriented Arakelov divisor $D = (I, u)$ is defined by the degree of the Arakelov divisor $(I, |u|)$. A *principal* oriented Arakelov divisor has the form $(f) = (f^{-1}O_F, f)$ for some $f \in F^*$ where the second part in its Hermitian line bundle is $f := (\sigma(f))_{\sigma} \in F_{\mathbb{R}}^*$. The set of oriented Arakelov divisors of degree 0 form a group denoted by $\widetilde{\text{Div}}_F^0$. It contains the subgroup of principal oriented divisors.

Definition 2.8. The quotient of the group $\widetilde{\text{Div}}_F^0$ by the subgroup of principal oriented divisors is called the *oriented Arakelov class group*. It is denoted by $\widetilde{\text{Pic}}_F^0$.

Let $F_{\mathbb{R}, \text{conn}}^*$ denote the connected component of $1 \in F_{\mathbb{R}}^*$. Then it is isomorphic to $\prod_{\sigma \text{ real}} \mathbb{R}_+^* \times \prod_{\sigma \text{ complex}} \mathbb{C}^*$. We denote by $F_+^* = \{f \in F^* : \sigma(f) > 0 \text{ for all real } \sigma\}$ and $O_{F,+}^* = \{\varepsilon \in O_F^* : \sigma(\varepsilon) > 0 \text{ for all real } \sigma\}$, subgroups of $F_{\mathbb{R}, \text{conn}}^*$ and put

$$(F_{\mathbb{R}, \text{conn}}^*)^0 = \{u \in F_{\mathbb{R}, \text{conn}}^* : N(u) = 1\} \quad \text{and} \quad \widetilde{T}^0 = (F_{\mathbb{R}, \text{conn}}^*)^0 / O_{F,+}^*.$$

The *narrow ideal class group* is a finite group defined as $Cl_{F,+} = Id_F / \{fO_F : f \in F_+^*\}$.

The following proposition says that the groups \widetilde{T}^0 is the connected components of identity of $\widetilde{\text{Pic}}_F^0$. It provides an analogue to Proposition 2.6.

Proposition 2.9. *The natural sequence below is exact.*

$$0 \longrightarrow \widetilde{T}^0 \longrightarrow \widetilde{\text{Pic}}_F^0 \longrightarrow Cl_{F,+} \longrightarrow 0$$

Proof. See [7, Proposition 5.3]. □

By Dirichlet's unit theorem, \widetilde{T}^0 is a compact torus of dimension $n - 1$ [8, Section 4.9]. For $u \in F_{\mathbb{R}}^*$, let y denote the element $y = \log u := (\log(u_{\sigma}))_{\sigma} \in \prod_{\sigma} F_{\sigma} = F_{\mathbb{R}}$. Here we use the principal branch of the complex logarithm. Then we define

$$\|u\|_{\widetilde{Pic}}^2 := \min_{\varepsilon \in O_{F,+}^*} \|\log(\varepsilon u)\|^2 = \min_{\varepsilon \in O_{F,+}^*} \sum_{\sigma} \deg(\sigma) |\log(u_{\sigma} \sigma(\varepsilon))|^2.$$

Let two divisor classes D and D' that lie on the same connected component of $\widetilde{\text{Pic}}_F^0$. By Proposition 2.9, there is some unique $u \in \widetilde{T}^0$ such that $D - D' = (O_F, u)$. We define the *distance* between two classes of D and D' as $\|u\|_{\widetilde{Pic}}$. The function $\| \cdot \|_{\widetilde{Pic}}$ gives rise to a distance function that induces the natural topology of $\widetilde{\text{Pic}}_F^0$. So, $\widetilde{\text{Pic}}_F^0$ is in this way equipped with a translation invariant Riemannian structure [7, Section 6].

3. STRONGLY C -REDUCED ARAKELOV DIVISORS

The purpose of this section is to introduce strongly C -reduced Arakelov divisors of a number field F and to demonstrate some examples. See Chapter 3 in [9] for more details.

Definition 3.1. Let I be a fractional ideal. Then 1 is called *primitive* in I if $1 \in I$ and it is not divisible by any integer $d \geq 2$.

Definition 3.2. Let $C \geq 1$. A fractional ideal I is called *strongly C -reduced* if the following hold:

- $1 \in I$ is primitive and
- For all $g \in I \setminus \{0\}$, we have $\|1\| \leq C\|g\|$.

The second condition can be restated as follows: the shortest vector of the lattice I has length at least $\frac{\sqrt{n}}{C}$. In other words, let S be the sphere centered at the origin and radius $\frac{\sqrt{n}}{C}$. Then the interior of S does not contain any nonzero points of the lattice I . Observe that if I is strongly C -reduced then I is strongly C' -reduced for any $C' \geq C$.

Example 3.1. Let $F = \mathbb{Q}(\sqrt{7})$. Then $n = 2$ and the ring of integers of F is $O_F = \mathbb{Z}[\sqrt{7}]$. Let $I = O_F + \alpha O_F$ with $\alpha = \frac{1+\sqrt{7}}{4}$. Then 1 is primitive in I . The vector α is a shortest vector of the lattice I with length $\|\alpha\| = 1$. If $C = 1$, then the interior of the circle centered at the origin and radius $\sqrt{n}/C = \sqrt{2}$ contains α , hence I is not strongly C -reduced. In case $C = 2$, the interior of the circle centered at the origin and radius $\sqrt{n}/C = \frac{\sqrt{2}}{2}$ does not contain any nonzero points of the lattice I , so I is strongly C -reduced. (See Figure 1 and Figure 2).

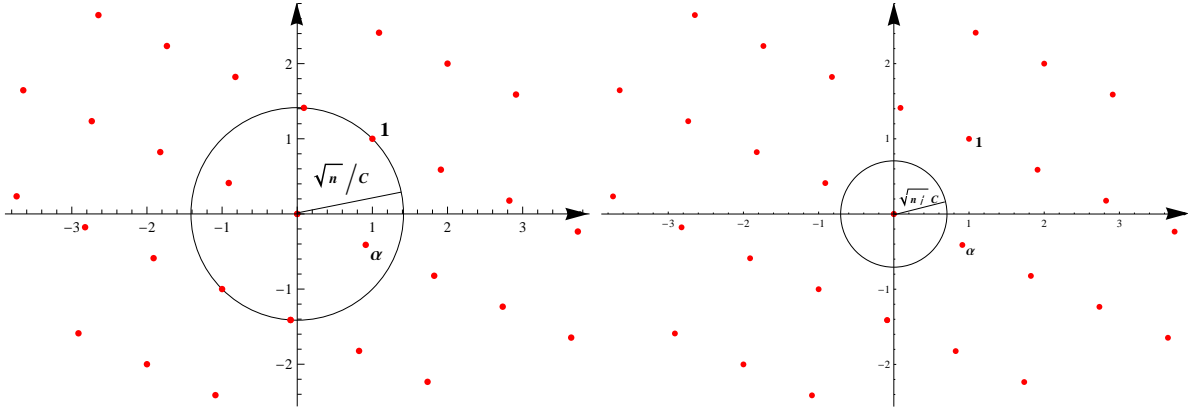


FIGURE 1. $C = 1$: I is not strongly C -reduced.

FIGURE 2. $C = 2$: I is strongly C -reduced.

Definition 3.3. An Arakelov divisor D is called *strongly C -reduced* if D has the form $D = d(I)$ for some strongly C -reduced fractional ideal I .

Example 3.2. Let F be a number field of degree n and let I be a fractional ideal of F .

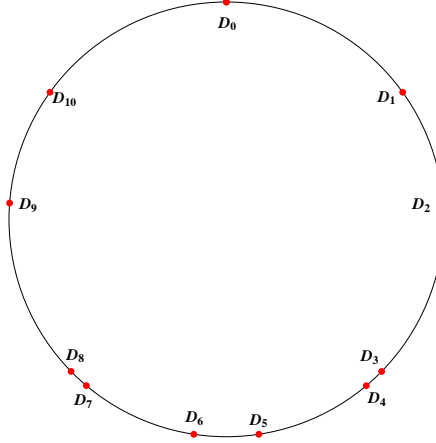


FIGURE 3. Strongly C -reduced Arakelov divisors of $\mathbb{Q}(\sqrt{73})$ with $C = \sqrt{2}$.

- If 1 is the shortest vector of the lattice I , then $d(I)$ is strongly C -reduced with $C = 1$. In particular, $D = (O_F, 1)$ is strongly 1-reduced.
- If I is reduced in the usual sense, in other words if 1 is minimal in I (see Section 2.1 or see Section 7 in [7]), then $d(I)$ is strongly C -reduced with $C = \sqrt{n}$.
- Let $F = \mathbb{Q}(\sqrt{\Delta})$ be a real quadratic field with $\Delta = 73$. There are totally 11 strongly C -reduced Arakelov divisors on the principal circle T^0 of Pic_F^0 with $C = \sqrt{2}$. They are symmetric through the vertical line passing D_0 (see Figure 3). Moreover, nine divisors are reduced in the usual sense and two divisors D_3, D_8 are strongly C -reduced with $C = \sqrt{2}$ but not reduced in the usual sense (see [7]).
- Let b_1, \dots, b_n be an LLL-reduced basis of I and let $J = b_1^{-1}I$. Assume that 1 is primitive in J . Then $d(J)$ is strongly C -reduced with $C = 2^{(n-1)/2}\sqrt{n}$ (see [5] and [9, Chapter 3]).

4. PROPERTIES OF STRONGLY C -REDUCED ARAKELOV DIVISORS

In this section, let F be a number field of degree n admitting r_1 real infinite primes and r_2 complex infinite primes. Denote by $\partial_F = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta|}$. We first claim that the set $Sred_F^C$ of all strongly C -reduced divisors are regularly distributed in the topological groups Pic_F^0 as well as in $\widetilde{\text{Pic}}_F^0$. Then we bound for its cardinality.

We first recall the lemma below.

Lemma 4.1. *Let $D = (I, u)$ be a divisor of degree 0. Then there is a nonzero element $f \in I$ such that $u_\sigma |\sigma(f)| \leq \partial_F^{1/n}$ for all σ . In particular, we obtain that $\|f\|_D \leq \sqrt{n} \partial_F^{1/n}$.*

Proof. See [7, Proposition 4.4]. □

Lemma 4.2. *Let $D = (I, u)$ be a divisor of degree 0. Then there is a minimal element $f \in I$ such that $u_\sigma |\sigma(f)| \leq \partial_F^{1/n}$ for all σ .*

Proof. Since $D = (I, u)$ is an Arakelov divisors of degree 0, by Lemma 4.1, there is a nonzero element g in I such that

$$(4.1) \quad u_\sigma |\sigma(g)| \leq \partial_F^{1/n} \text{ for all } \sigma.$$

We claim that there is a minimal element f of I satisfying this condition. Indeed, if g is minimal then we are done. If g is not minimal then the box $S_g = \{f \in I : |\sigma(f)| < |\sigma(g)| \text{ for all } \sigma\}$ contains some nonzero element f_1 of I . Hence $u_\sigma |\sigma(f_1)| \leq \partial_F^{1/n}$ for all σ . In other words, we can replace g by f_1 in (4.1). If f_1 is minimal then we are done. If not then there is some nonzero element f_2 in S_{f_1} satisfying (4.1) and so on. Since the box S_g is bounded, it only contains finitely many elements of the lattice I . Therefore, after finite steps, we can find a minimal element f of I satisfying $u_\sigma |\sigma(f)| \leq \partial_F^{1/n}$ for all σ . This proves the claim. \square

The following proposition says that the set of all strongly C -reduced Arakelov divisors of a number field is finite. It is similar to Proposition 7.2 in [7].

Proposition 4.3. *Let I be a fractional ideal. If $d(I)$ is a strongly C -reduced Arakelov divisor, then the inverse I^{-1} of I is an integral ideal and its norm is at most $C^n \partial_F$. In particular, the set $Sred_F^C$ of all strongly C -reduced Arakelov divisors is finite.*

Proof. Since $1 \in I$, it follows that $I^{-1} \subset O_F$. By Lemma 4.1, there is a nonzero element $f \in I$ such that

$$\|N(I)^{-1/n} f\| \leq \sqrt{n} \partial_F^{1/n}.$$

The divisor $d(I)$ is strongly C -reduced, thus $\|f\| \geq \frac{\sqrt{n}}{C}$. Consequently, the following is derived.

$$N(I^{-1}) \leq \frac{\sqrt{n}^n \partial_F}{\|f\|^n} \leq \frac{\sqrt{n}^n \partial_F}{\left(\frac{\sqrt{n}}{C}\right)^n} = C^n \partial_F.$$

Since the number integral ideals of bounded norm is finite, so is the set of all C -reduced Arakelov divisors $Sred_F^C$. \square

We first recall the lemma below [7, Lemma 7.5].

Lemma 4.4. *Let $x_i \in \mathbb{R}$ for $i = 1, 2, \dots, n$. Suppose that $\sum_{i=1}^n x_i = 0$ and that $x \in \mathbb{R}$ has the property that $x_i \leq x$ for all $i = 1, 2, \dots, n$ then $\sum_{i=1}^n x_i^2 \leq n(n-1)x^2$.*

Since this lemma can be proved easily by induction on n , we skip the proof here.

The case $C > \sqrt{n}$ is presented by the following theorem. Its result and proof are the same as Theorem 7.4 in [7]. The reason is that if a fractional ideal is reduced in the usual sense, then it is strongly C -reduced with $C \geq \sqrt{n}$.

Theorem 4.5. *Let $C \geq \sqrt{n}$. Then for any Arakelov divisor $D = (I, u)$ of degree 0, there is a strongly C -reduced divisor D' lying on the same connected component of Pic_F^0 as D for which $\|D - D'\|_{\text{Pic}} < \log \partial_F$.*

Proof. See the proof of Theorem 7.4 in [7]. \square

Theorem 4.6. *Let $1 < C \leq \sqrt{n}$. Then for any Arakelov divisor $D = (I, u)$ of degree 0, there is a strongly C -reduced divisor D' lying on the same connected component of Pic_F^0 as D and*

$$\|D - D'\|_{\text{Pic}} < \frac{\log n}{2 \log C} \log \partial_F.$$

Proof. By Lemma 4.2, there is a minimal element f in I such that

$$(4.2) \quad u_\sigma |\sigma(f)| \leq \partial_F^{1/n} \text{ for all } \sigma.$$

Let $J_1 = f^{-1}I$ and $D_1 = d(J_1)$. Then 1 is minimal in J_1 and J_1^{-1} is an integral ideal with $1 \leq N(J_1^{-1}) \leq \partial_F$. See Section 7 in [7]. It is divided into two cases as below.

Case 1: $\|1\| \leq C\|f_1\|$ where f_1 is the shortest vector of J_1 . Then D_1 is strongly C -reduced. Note that 1 is minimal and hence primitive in J_1 . We choose $D' = D_1$. Then

$$D - D' + (f) = (O_F, v_1) \text{ with } v_1 = uN(J_1)^{1/n}|f|.$$

The divisor D' is on the same connected component of Pic_F^0 as D and $v_{1\sigma} = u_\sigma |\sigma(f)| N(J_1)^{1/n}$ for all σ . Hence,

$$\log v_{1\sigma} = \log u_\sigma |\sigma(f)| + \log N(J_1)^{1/n} \leq \log u_\sigma |\sigma(f)| \text{ for all } \sigma.$$

The second inequality holds because $N(J_1) \leq 1$. By choosing f , each $\log v_{1\sigma}$ is bounded by $\log \partial_F^{1/n}$ for all σ . In addition, since $\sum_\sigma \log v_{1\sigma} = 0$, Lemma 4.4 indicates that

$$\|\log v_1\|^2 \leq n(n-1) \left(\log \partial_F^{1/n} \right)^2$$

and so

$$\|D - D'\|_{\text{Pic}} = \|v_1\|_{\text{Pic}} \leq \|v_1\|_{\text{Pic}} < \log \partial_F \leq \frac{\log n}{2 \log C} \log \partial_F.$$

Case 2: $\|1\| > C\|f_1\|$. Assume that $k \geq 1$ is the largest integer for which the shortest vector f_j of the lattice J_j has the property that $\|1\| > C\|f_j\|$ for all $1 \leq j \leq k$ where $J_1 = f^{-1}I$ and $J_i = f_{i-1}^{-1}J_{i-1}$ if $2 \leq i \leq k$. We claim that k is bounded.

Indeed, let $J_{k+1} = f_k^{-1}J_k$. The arithmetic geometric mean inequality says that $|N(f_j)| \leq n^{-n/2} \|f_j\|^n < \frac{1}{C^n}$ for $1 \leq j \leq k$ [7, Proposition 3.1].

$$N(J_{k+1}^{-1}) = N(f_k \cdots f_1 J_1^{-1}) = |N(f_k)| \cdots |N(f_1)| N(J_1^{-1}) < \frac{1}{C^{nk}} N(J_1^{-1}) \leq \frac{\partial_F}{C^{nk}}.$$

Since J_{k+1}^{-1} is an integral ideal, we obtain that $N(J_{k+1}^{-1}) \geq 1$. This and the previous inequality imply that $C^{nk} < \partial_F$. Thus, $k < \frac{\log \partial_F}{n \log C}$.

Because of the property of k , the divisor $D_{k+1} = d(J_{k+1})$ is strongly C -reduced. Moreover, let $D' = D_{k+1}$. Then D' is on the same connected component of Pic_F^0 as D and

$$D - D' + (f_k \cdots f_2 f_1 f) = (O_F, v_{k+1}).$$

Here $v_{k+1} = uN(J_{k+1})^{1/n}|f_k \cdots f_1 f|$ and $\|f_j\| \leq \frac{\sqrt{n}}{C}$ for all $j = 1, \dots, k$. Then using an argument similar to the first case, we obtain that

$$v_{k+1,\sigma} \leq \|f_k\| \cdots \|f_1\| u_\sigma |\sigma(f)| N(J_{k+1})^{1/n} \leq \left(\frac{\sqrt{n}}{C}\right)^k \partial_F^{1/n} \text{ for all } \sigma,$$

and so

$$\|D - D'\|_{Pic} = \|v_{k+1}\|_{Pic} < kn \log \frac{\sqrt{n}}{C} + \log \partial_F < \frac{\log n}{2 \log C} \log \partial_F.$$

The second inequality comes from the fact that $k < \frac{\log \partial_F}{n \log C}$. Thus, the proposition is proved. \square

Remark 4.7. Note that Theorem 4.5 and 4.6 agree on the case $C = \sqrt{n}$. In case $C = 1$, using the same notations and a similar argument as in the proof of Theorem 4.6 leads to the following result.

$$\|D - D'\|_{Pic} < (\text{some constant}) \cdot \sqrt{|\Delta_F|}.$$

Currently, determining whether the distance from D' to D is bounded above by a polynomial in $\log \partial_F$ is still an open problem.

The second theorem is a new version of Theorem 7.7 in [7] for strongly C -reduced divisors. It says that the set of strongly C -reduced divisors is quite sparse in $\widetilde{\text{Pic}}_F^0$. Explicitly, the distance between two distinct strongly C -reduced Arakelov divisors lying on the same component of $\widetilde{\text{Pic}}_F^0$ is at least $\log \left(1 + \frac{\sqrt{3}}{2C^2}\right)$. This distance depends on C but not on the number field.

Theorem 4.8. *Let $C \geq 1$ and let $\delta = \log \left(1 + \frac{\sqrt{3}}{2C^2}\right)$. Then we have the following.*

- (i) *Let D and D' be two strongly C -reduced Arakelov divisors in $\widetilde{\text{Div}}_F^0$. If there exists an element $f \in F_+^*$ for which $D - D' + (f) = (O_F, v)$ with $|\log v_\sigma| < \delta$ for each σ then $D = D'$ in $\widetilde{\text{Div}}_F^0$.*

In particular, if $\|v\|_{\widetilde{\text{Pic}}_F} < \delta$, then $D = D'$ in $\widetilde{\text{Div}}_F^0$.

- (ii) *The natural map from*

$$\bigcup_{D \in \text{Sred}_F^C} \{D + (O_F, v) : v \in (F_{\mathbb{R}, \text{conn}}^*)^0 \text{ and } |\log v_\sigma| < \tfrac{1}{2}\delta \text{ for each } \sigma\}$$

to $\widetilde{\text{Pic}}_F^0$ is injective.

Proof.

- (i) Suppose that $D = d(I)$ and $D' = d(I')$ are two strongly C -reduced divisors with $D - D' + (f) = (O_F, v)$ for some $f \in F^*$ such that $\sigma(f) > 0$ for all real σ . So, the images of D and D' lie on the same connected component of $\widetilde{\text{Pic}}_F^0$. It also implies that $\|D - D'\|_{\widetilde{\text{Pic}}_F} = \|v\|_{\widetilde{\text{Pic}}_F}$ and $I = fI'$.

Let $\lambda = N(I/I')^{\frac{1}{n}} = |N(f)|^{\frac{1}{n}}$. By changing I and I' if necessary, we can assume that $\lambda \leq 1$. Then $v = N(I/I')^{-\frac{1}{n}} f = \frac{1}{\lambda} f$. Therefore, $\frac{\sigma(f)}{\lambda} = v_\sigma$ and $|\log v_\sigma| < \delta$ for all σ . In consequence, we have the following.

$$|\sigma(f)/\lambda - 1| = |v_\sigma - 1| = |\exp(\log v_\sigma) - 1| = \exp|\log(v_\sigma)| - 1 < e^\delta - 1.$$

The assumption $\lambda \leq 1$ leads to $|\sigma(f) - \lambda| < (e^\delta - 1)\lambda \leq e^\delta - 1$ for every σ . Thus $\|f - \lambda \cdot 1\| < \sqrt{n}(e^\delta - 1)$.

Suppose that 1 and f are \mathbb{R} -linearly independent then $L = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot f \subset F_{\mathbb{R}}$ is a lattice of rank 2. And let $d(f, \mathbb{R} \cdot 1)$ denote the distance from f to $\mathbb{R} \cdot 1$, the 1-dimensional subspace of $F_{\mathbb{R}}$ spanned by 1. Since

$$d(f, \mathbb{R} \cdot 1) \leq \|f - \lambda \cdot 1\| < \sqrt{n}(e^\delta - 1),$$

the lattice L has covolume

$$\text{covol}(L) = \|1\| \cdot d(f, \mathbb{R} \cdot 1) < n(e^\delta - 1).$$

On the other hand, L contains a nonzero element g such that

$$\|g\|^2 \leq \left(\frac{4}{3}\right)^{1/2} \text{covol}(L)$$

[5, Section 9]. As a result, we obtain that

$$\|g\|^2 < \frac{2}{\sqrt{3}} n(e^\delta - 1).$$

Both 1 and f are in I , so then g . By assumption, $D = d(I)$ is strongly C -reduced, hence $\|g\| \geq \sqrt{n}/C$ and

$$\frac{n}{C^2} \leq \|g\|^2 < \frac{2}{\sqrt{3}} n(e^\delta - 1) = \frac{n}{C^2}.$$

This contradiction follows from the assumption that 1 and f are \mathbb{R} -linearly independent. Therefore, 1 and f are \mathbb{R} -linearly dependent. Then there is some $r \in \mathbb{R}$ for which $\sigma(f) = r \cdot 1 = r$ for all σ . This implies that $f \in \mathbb{Q}$. Since 1 is primitive in I and $f \in I$, we must have $f \in \mathbb{Z}$. Accordingly, $|f| = |N(f)|^{\frac{1}{n}} = \lambda \leq 1$. As a result, $f = \pm 1$ and $I = I'$. It follows that $D = D'$ in \widetilde{Div}_F^0 . That completes the proof of the first part in (i).

In particular, if $\|v\|_{\widetilde{Pic}} < \delta$, then $\min_{\varepsilon \in O_{F,+}^*} \|\log(v\varepsilon)\| < \delta$. Consequently, there is some element $\varepsilon \in O_F^*$ for which $\sigma(\varepsilon) > 0$ for all real σ and $|\log(v_\sigma \sigma(\varepsilon))| < \delta$ for all σ . Replacing f by $\varepsilon f \in F_+^*$, the following is obtained.

$$D - D' = (\varepsilon f) + (O_F, v\varepsilon) \text{ and } |\log(v_\sigma \sigma(\varepsilon))| < \delta \text{ for each } \sigma.$$

Then the result follows by applying the first statement in (i), which is proved above.

(ii) Assume that two divisors $D_1 = D + (O_F, v_1)$ and $D_2 = D' + (O_F, v_2)$ are in the left set in (ii) and have the same image in \widetilde{Pic}_F^0 . Then D and D' are strongly C -reduced divisors, $v_1 = (v_{1\sigma})_\sigma$ and $v_2 = (v_{2\sigma})_\sigma$ are in $(F_{\mathbb{R}, conn}^*)^0$ satisfying $|\log v_{1\sigma}| < \frac{1}{2}\delta$ and $|\log v_{2\sigma}| < \frac{1}{2}\delta$ for all σ . Moreover, $D_1 - D_2 = (f^{-1}O_F, f) = (f)$ for some $f \in F_+^*$.

Thus, $D - D' = (f) + (O_F, v)$ where $f \in F_+^*$ and $v = v_1 v_2^{-1}$. In addition, $|\log v_\sigma| = |\log v_{1\sigma} - \log v_{2\sigma}| < \frac{1}{2}\delta + \frac{1}{2}\delta = \delta$ for all σ . By part (i), two divisors D and D' must coincide in \widetilde{Div}_F^0 . As a sequence, $(f^{-1}O_F, f) = (O_F, v)$ in \widetilde{Div}_F^0 . Therefore, $f \in O_F^*$ and so $D_1 = D_2$. This claims that the map in (ii) is injective. \square

Theorem 4.8 has the following corollary.

Corollary 4.9. *Let $C \geq 1$. Then the number of strongly C -reduced Arakelov divisors contained in a ball of radius 1 in Pic_F^0 is at most $(\frac{1}{2} \log(1 + \frac{3}{2C^2}))^{-n}$.*

Proof. We denote $\log(1 + \frac{3}{2C^2})$ briefly by δ . Let B be a ball of radius 1 in Pic_F^0 . And let $B_R = B \cap \text{Sred}_F^C$ be the set of strongly C -reduced divisors whose images are contained in B . Then B_R is contained in a subset S of $\widetilde{\text{Pic}}_F^0$ of volume $\frac{2^{r_1}(2\pi\sqrt{2})^{r_2}}{\omega_F}$ times the volume of a unit ball in Pic_F^0 .

For each strongly C -reduced divisor D in B_R , we denote by $B_{1/2\delta}(D)$ the ball of radius $\frac{1}{2}\delta$ centered at D in $\widetilde{\text{Pic}}_F^0$. By Theorem 4.8, these balls are mutually disjoint in S . Therefore, the followings holds.

$$\sum_{D \in B_R} \text{vol}(B_{1/2\delta}(D)) \leq \text{vol}(S).$$

Each ball $B_{1/2\delta}(D)$ has volume equal to the volume of the ball $B_{1/2\delta}$ centered at the origin and radius $1/2\delta$ in $\widetilde{\text{Pic}}_F^0$. Hence

$$\#B_R \cdot \text{vol}(B_{1/2\delta}) \leq \text{vol}(S).$$

Besides, the balls $B_{1/2\delta}$ have covolume $\frac{2^{r_1}(2\pi\sqrt{2})^{r_2}}{\omega_F} (\frac{1}{2}\delta)^n$ times the volume of a unit ball in Pic_F^0 . This leads to the following.

$$\#B_R \leq \frac{\text{vol}(S)}{\text{vol}(B_{1/2\delta})} = \left(\frac{1}{\frac{1}{2}\delta}\right)^n = \left(\frac{1}{2}\delta\right)^{-n}.$$

So, the corollary is proved. \square

Finally, we bound for $\#\text{Sred}_F^C$ as below.

Corollary 4.10. *Let $C \geq 1$. Then*

$$\#\text{Sred}_F^C \leq 2^n \left(\log \left(1 + \frac{3}{2C^2} \right) \right)^{-n/2} \text{vol}(\widetilde{\text{Pic}}_F^0).$$

Proof. Let S be the simplex given by

$$S = \{v \in (F_{\mathbb{R}, \text{conn}})^0 : |\log v_\sigma| < \frac{1}{2}\delta \text{ for all } \sigma\}.$$

Then its volume is

$$\text{vol}(S) = \frac{2^{-r_2/2} n^{r_1+r_2-1/2}}{(r_1+r_2-1)!} \left(\frac{1}{2}\delta\right)^{r_1+r_2} \geq 2^{-n} \delta^{n/2}.$$

Furthermore, the second part of Theorem 4.8 implies that

$$\mathrm{vol}(\widetilde{\mathrm{Pic}}_F^0) \geq \#Sred_F^C \cdot \mathrm{vol}(S).$$

Therefore, the result follows. \square

ACKNOWLEDGEMENT

I would like to thank Hendrik W. Lenstra for helping me to prove Theorem 4.8 and René Schoof for very useful comments. The author also would like to thank the reviewers for their comments that helped improve the manuscript. I would also like to show my gratitude to the Mathematics department at the University of Leiden for its hospitality during the fall 2013.

This research was supported by the Università di Roma “Tor Vergata”. The author is financially supported by the Academy of Finland grants #276031, #282938 and #283262. The support from the European Science Foundation under the COST Action IC1104 is also gratefully acknowledged.

REFERENCES

- [1] Eva Bayer-Fluckiger. Lattices and number fields. In *Algebraic geometry: Hirzebruch 70 (Warsaw, 1998)*, volume 241 of *Contemp. Math.*, pages 69–84. Amer. Math. Soc., Providence, RI, 1999.
- [2] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41. Birkhäuser Boston, Boston, MA, 1990.
- [3] Johannes Buchmann and H. C. Williams. On the infrastructure of the principal ideal class of an algebraic number field of unit rank one. *Math. Comp.*, 50(182):569–579, 1988.
- [4] H. W. Lenstra, Jr. On the calculation of regulators and class numbers of quadratic fields. In *Number theory days, 1980 (Exeter, 1980)*, volume 56 of *London Math. Soc. Lecture Note Ser.*, pages 123–150. Cambridge Univ. Press, Cambridge, 1982.
- [5] Hendrik W. Lenstra, Jr. Lattices. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 127–181. Cambridge Univ. Press, Cambridge, 2008.
- [6] R. J. Schoof. Quadratic fields and factorization. In *Computational methods in number theory, Part II*, volume 155 of *Math. Centre Tracts*, pages 235–286. Math. Centrum, Amsterdam, 1982.
- [7] René Schoof. Computing Arakelov class groups. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 447–495. Cambridge Univ. Press, Cambridge, 2008.
- [8] Daniel Shanks. The infrastructure of a real quadratic field and its applications. In *Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972)*, pages 217–224. Univ. Colorado, Boulder, Colo., 1972.
- [9] Ha T. N. Tran. On reduced arakelov divisors of a number field. Doctoral Thesis, University of Rome Tor Vergata, 2015.
- [10] Ha T. N. Tran. On reduced arakelov divisors of real quadratic fields, to appear in *Acta Arith.*
- [11] Hugh C. Williams. Continued fractions and number-theoretic computations. *Rocky Mountain J. Math.*, 15(2):621–655, 1985. Number theory (Winnipeg, Man., 1983).

DEPARTMENT OF MATHEMATICS AND SYSTEMS ANALYSIS, AALTO UNIVERSITY SCHOOL OF SCIENCE, OTAKAARI 1, 02150 ESPOO, FINLAND.

E-mail address: hatran1104@gmail.com